

特開平7-182142

(43) 公開日 平成7年(1995)7月21日

(51) Int.Cl.⁶

識別記号

庁内整理番号

F I

技術表示箇所

G 0 6 F 7/52

A

審査請求 未請求 請求項の数 4 F D (全 7 頁)

(21) 出願番号 特願平5-346646

(22) 出願日 平成5年(1993)12月22日

(71) 出願人 000001007

キヤノン株式会社

東京都大田区下丸子3丁目30番2号

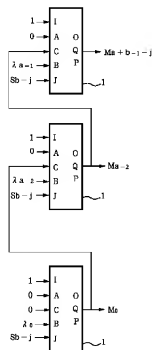
(72) 発明者 岩村 恵市

東京都大田区下丸子3丁目30番2号 キヤ
ノン株式会社内

(74) 代理人 弁理士 渡部 敏彦

(54) 【発明の名称】 多項式乗算回路

(57) 【要約】

【目的】 $\lambda(x)$ の係数が一括して入力される場合でも有効に乗算を行える多項式乗算回路を提供する。【構成】 本回路は、第1の入力と第2及び第3の入力の積との和を出力する複数の演算素子1をa個縦に配列したものである。複数の演算素子1を1次元状のアレイで構成することにより、 x^na を法としない一般的な多項式の乗算を連続して実行することができ、 $\lambda(x)$ の係数が一括して入力される場合でも有効に乗算を行える。

1

【特許請求の範囲】

【請求項1】 第1の入力と第2及び第3の入力の積との和を出力する演算素子をa個配列し、i番目に配列した前記演算素子において、1+1番目に配列した前記演算素子の出力を前記第1の入力とし、与えられたa-1次の多項式 $\lambda(x)$ のa-1次の係数を前記第2の入力とし、与えられたb-1次の多項式 $S(x)$ の係数を高次の係数から順次前記第3の入力とすることにより、

$$M(x) = \lambda(x) \cdot S(x)$$

を展開した多項式の係数を、前記演算素子の出力として得ることを特徴とする多項式乗算回路。

【請求項2】 i番目の前記演算素子の出力を、

$$M(x) = \lambda(x) \cdot S(x) \bmod X^a$$

(ここで“ \bmod ”は、その直後の数式が累乗数であることを示している)を展開した多項式の X^{a-1} の係数として得ることを特徴とする請求項1記載の多項式乗算回路。

【請求項3】 第1の入力と第2及び第3の入力の積との和を出力する演算素子をa個配列し、i番目に配列した前記演算素子において、1+1番目に配列した前記演算素子の出力を前記第1の入力とし、与えられたa-1次の多項式 $\lambda(x)$ のi-1次の係数を前記第2の入力とし、与えられたb-1次の多項式 $S(x)$ の係数を高次の係数から順次前記第3の入力とすることにより、

$$M(x) = \lambda(x) \cdot S(x)$$

を展開した多項式の係数を、前記演算素子の出力として得ることを特徴とする多項式乗算回路。

【請求項4】 i番目の前記演算素子の出力を、

$$M(x) = \lambda(x) \cdot S(x) / x^{b-2}$$

を展開した多項式の係数として得ることを特徴とする請求項3記載の多項式乗算回路。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は光ディスクや光磁気ディスク等のデータ記憶媒体や、衛星通信等のデータ通信の通信路におけるデータの誤りを訂正するための誤り訂正符号であるリード・ソロモン符号(以下、「RS符号」と略す。)のような符号処理に好適な多項式乗算回路に関する。

【0002】

【従来の技術】 近年、光ディスク等の記憶媒体を用いたメモリーシステムをはじめとする各種デジタル・システムの情報性向上のために、誤り訂正符号を用いた誤り訂正方法の利用が浸透してきている。特に、このような符号としては、RS符号が、同一の符号長と訂正能力を持つ符号の中で、最も冗長度を小さくできるという実用上重要な特徴を持つため、光ディスクや光磁気ディスク、衛星通信等で広く用いられている。

【0003】 ところで、RS符号の復号器は、訂正能力が1又は2程度と小さい場合は、比較的容易に装置が構

2

成できるが、訂正能力を大きくした場合、装置の規模が大きくなり、制御も非常に複雑になり、復号処理に要する時間も大きくなってしまった問題があった。

【0004】 そこで、並列処理回路の一つであるシストリックアレイを用いた誤り訂正方式が提案されている。それによれば、RS符号の復号に必要なすべての処理を積和演算 $a \cdot b + c \cdot d$ に分解し、この演算を同型のプロセッシング・エレメント(PE)により実行するようにして、このPE1を図6に示すように複数個並べたアレイを利用することにより、多項式 $\lambda(x)$ と $S(x)$ の x^a を法とする乗算

$$M(x) = \lambda(x) \cdot S(x) \bmod x^a$$

を簡単な制御により計算し、高速処理が実現されるというものである。なお、図4においてA、C、B、I、J、O、P、Qは、プロセッシングエレメントを示す。

【0005】

【発明が解決しようとする課題】 しかしながら、上述のシストリックアレイは、 $\lambda(x)$ の係数入力にシリアルに行われる場合に対してのみ有効であり、 $\lambda(x)$ の係数が一括して入力される場合には有効ではなかった。

【0006】 そこで、本発明は、上記事情に鑑みてなされたものであり、 $\lambda(x)$ の係数が一括して入力される場合でも有効に乗算を行える多項式乗算回路を提供することを目的とする。

【0007】

【課題を解決するための手段】 上記目的を達成するために請求項1記載の多項式乗算回路は、第1の入力と第2及び第3の入力の積との和を出力する演算素子をa個配列し、i番目に配列した前記演算素子において、1+1番目に配列した前記演算素子の出力を前記第1の入力とし、与えられたa-1次の多項式 $\lambda(x)$ のa-1次の係数を前記第2の入力とし、与えられたb-1次の多項式 $S(x)$ の係数を高次の係数から順次前記第3の入力とすることにより、

$$M(x) = \lambda(x) \cdot S(x)$$

を展開した多項式の係数を、前記演算素子の出力として得ることを特徴とするものである。

【0008】 また、請求項2記載の多項式乗算回路は、i番目の前記演算素子の出力を、

$$M(x) = \lambda(x) \cdot S(x) \bmod X^a$$

を展開した多項式の X^{a-1} の係数として得ることを特徴とするものである。

【0009】 また、請求項3記載の多項式乗算回路は、第1の入力と第2及び第3の入力の積との和を出力する演算素子をa個配列し、i番目に配列した前記演算素子において、1+1番目に配列した前記演算素子の出力を前記第1の入力とし、与えられたa-1次の多項式 $\lambda(x)$ のi-1次の係数を前記第2の入力とし、与えられたb-1次の多項式 $S(x)$ の係数を高次の係数から順次前記第3の入力とすることにより、

3

$$M(x) = \lambda(x) \cdot S(x)$$

を展開した多項式の係数を、前記演算素子の出力として得ることを特徴とするものである。

【0010】また、請求項4記載の多項式乗算回路は、1番目の前記演算素子の出力を、

$$M(x) = \lambda(x) \cdot S(x) / x^{b-2}$$

を展開した多項式の係数として得ることを特徴とするものである。

【0011】

【作用】請求項1記載の多項式乗算回路によれば、複数の演算素子を1次元状のアレイで構成することにより、 x^a を法としない一般的な多項式の乗算を連続して実行することができ、 $\lambda(x)$ の係数が一括して入力される場合でも有効に乗算を行える。

【0012】請求項2記載の多項式乗算回路によれば、複数の演算素子を1次元状のアレイで構成することにより、 x^a を法とする多項式の乗算を連続して実行することができ、 $\lambda(x)$ の係数が一括して入力される場合でも有効に乗算を行える。

【0013】請求項3記載の多項式乗算回路によれば、複数の演算素子を1次元状のアレイで構成することにより、 x^{b-2} での除算を含まない一般的な多項式を連続して実行することができ、 $\lambda(x)$ の係数が一括して入力される場合でも有効に乗算を行える。

【0014】請求項4記載の多項式乗算回路によれば、複数の演算素子を1次元状のアレイで構成することにより、 x^{b-2} での除算を含む多項式を連続して実行することができ、 $\lambda(x)$ の係数が一括して入力される場合でも有効に乗算を行える。

【0015】

【実施例】以下、本発明の実施例を図面を参照して詳述する。

【0016】図5は本発明の多項式乗算回路を構成する演算素子のブロック構成図である。

【0017】この演算素子1は、図面に示すように、セレクト2、第1の乗算器3a、第2の乗算器3b、加算器4、第1のレジスタ5a、第2のレジスタ5b及び第3のレジスタ5c等から構成される例えばプロセッシング・エレメント(PE)であり、第1の入力Cと第2及び第3の入力B、Jの積との和を出力するものである。また、このセレクト2は、制御信号S1、S2によって出力端子Xに入力C、出力端子Yに入力Bを選択するものである。

【0018】図1は本発明の多項式乗算回路の第1の実施例を示すブロック構成図である。

【0019】この第1の実施例の回路は、図面に示すように、前記演算素子1をa個縦に配列し、1番目に配列した演算素子1において、1+1番目に配列した演算素子1の出力を第1の入力Cとし、与えられたa-1次の多項式 $\lambda(x)$ のa-1次の係数を第2の入力Bとし、

4

与えられたb-1次の多項式 $S(x)$ の係数を高次の係数から順次第3の入力Jとなるように、各演算素子1間を接続し、 x^a を法としない一般的な多項式 $M(x) = \lambda(x) \cdot S(x)$ を演算するものである。なお、図面において、jは処理クロックを表す。

【0020】次に、第1の実施例の動作を説明する。

【0021】a-1次の多項式 $\lambda(x)$ のi次の計数を λ_i 、b-1次の多項式 $S(x)$ のj次の係数を S_j とすると、 $M(x) = \lambda(x) \cdot S(x)$ の多項式の乗算は、次のアルゴリズムに示すように、各演算素子1の出力がパイプライン的に次の演算素子1に送られて実行される。但し、 $M(x)$ のr次の係数を M_r とし、 M_r 、 $Z_{i,j}$ の初期値は0とする。

【0022】

```
FOR j=1 TO b
  FOR i=1 TO a
    zi,j = Zi-1,j-1 +  $\lambda_{a-1-i} \cdot S_{b-j}$ 
  NEXT
  Ma+b-1-j = Z1,j
NEXT
FOR i=2 TO a
  Ma-i = Z1,b
NEXT
```

この場合、1+1番目に配列した演算素子1の出力は、処理クロックに同期して1番目に配列した演算素子1の第1入力Cとしてフィードバック入力される。このとき、 $M(x)$ の高次の係数である $M_{a+b-1-j}$ ($j=1, \dots, b$)は、1番目に配列した演算素子1の出力として順次得られるが、それ以下の $M(x)$ の係数 M_{a-i} は、bクロック後に1番目に配列した演算素子1の出力として一括して得られる。

【0023】このように第1の実施例によれば、 $\lambda(x)$ の各係数が一括して入力される場合に対して有効な乗算回路が実現できる。また、この回路の制御や構成も全ての演算素子1に対して同じであり、規則的で簡単となり、VLSIに適したものとなる。また、上記の実施例に示した回路は、誤り訂正のためだけに限らず、一般の乗算に対しても有効となる。

【0024】図2は本発明の多項式乗算回路の第2の実施例を示すブロック構成図である。

【0025】この第2の実施例の回路は、図面に示すように、第1の実施例と同様に前記演算素子1をa個縦に配列し、1番目に配列した演算素子1において、1+1番目に配列した演算素子1の出力を第1の入力Cとし、与えられたa-1次の多項式 $\lambda(x)$ のa-1次の係数を第2の入力Bとし、与えられたb-1次の多項式 $S(x)$ の係数を高次の係数から順次第3の入力Jとするように、各演算素子1間を接続し、 x^a を法とする多項式 $M(x) = \lambda(x) \cdot S(x) \bmod x^a$ を演算するものである。

5

【0026】次に、第2の実施例の動作を説明する。
 【0027】 $a-1$ 次の多項式 $\lambda(x)$ の1次の係数を λ_1 、 $b-1$ 次の多項式 $S(x)$ のj次の係数を S_j をとすると、 $M(x) = \lambda(x) \cdot S(x) \bmod x^a$ の多項式の乗算は、次のアルゴリズムに示すように、各演算素子1の出力がパイプライン的に次の演算素子1に送られて実行される。但し、 $M(x)$ のr次の係数を M_r 、 $Z_{i,j}$ の初期値は0とする。

```

【0028】
FOR j=1 TO b
  FOR i=1 TO a
    Zi,j = Zi+1,j-1 +  $\lambda_{a-i-1} \cdot S_{b-j}$ 
  NEXT
NEXT
FOR i=1 TO a
  Ma-i = Zi,b
NEXT

```

本実施例と第1実施例との違いは、本実施例では $M(x)$ のa次の係数を必要としない、即ち、 $M(x) \bmod x^a$ の演算を実行していることである。第1実施例では $M(x)$ のa次未満の係数 M_{a-1} はbクロック後にi番目に配列した演算素子1の出力として一括して得られるので、本実施例は図1のi番目に配列した演算素子1の出力を M_{a-i} として表現している。但し、図2はbクロック後の出力を表し、それまでの図2の回路の動作は図1の回路の動作と同様である。

【0029】図3は本発明の多項式乗算回路の第3の実施例を示すブロック構成図である。

【0030】この第3の実施例の回路は、図4に示すように、第1の実施例と同様に前記演算素子1をa個縦に配列し、i番目に配列した演算素子1において、 $i+1$ 番目に配列した演算素子1の出力を第1の入力Cとし、与えられた $a-1$ 次の多項式 $\lambda(x)$ の $i-1$ 次の係数を第2の入力Bとし、与えられた $b-1$ 次の多項式 $S(x)$ の係数を高次の係数から順次第3の入力Jとなるように、各演算素子1間を接続し、 X^{b-2} での除算を含まない一般的な多項式 $M(x) = \lambda(x) \cdot S(x)$ を演算するものである。

【0031】次に、第3の実施例の動作を説明する。

【0032】 $a-1$ 次の多項式 $\lambda(x)$ の1次の係数を λ_1 、 $b-1$ 次の多項式 $S(x)$ のj次の係数を S_j とすると、 $M(x) = \lambda(x) \cdot S(x)$ の多項式の乗算は、次のアルゴリズムに示すように、各演算素子1の出力がパイプライン的に次の演算素子1に送られて実行される。但し、 $M(x)$ のr次の係数を M_r とし、 M_r 、 $Z_{i,j}$ の初期値は0とする。

【0033】

6

```

FOR j=1 TO b
  FOR i=1 TO a
    Zi,j = Zi+1,j-1 +  $\lambda_{a-i-1} \cdot S_{b-j}$ 
  NEXT
  Mj-1 = Z1,j
NEXT
FOR i=2 TO a
  Mb-2+i = Zi,b
NEXT

```

10 この場合、 $i+1$ 番目に配列した演算素子1の出力は処理クロックに同期して1番目に配列した演算素子1の第1入力Cとしてフィードバック入力される。このとき、 $M(x)$ の低次の係数である M_{j-1} ($j=1, \dots, b$)は、1番目に配列した演算素子1の出力として順次得られるが、それ以上の $M(x)$ の係数である M_{b-2+i} は、bクロック後にi番目に配列した演算素子1の出力として一括して得られる。

【0034】図4は本発明の多項式乗算回路の第4の実施例を示すブロック構成図である。

20 【0035】この第3の実施例の回路は、図4に示すように、第1の実施例と同様に前記演算素子1をa個縦に配列し、i番目に配列した演算素子1において、 $i+1$ 番目に配列した演算素子1の出力を第1の入力Cとし、与えられた $a-1$ 次の多項式 $\lambda(x)$ の $i-1$ 次の係数を第2の入力Bとし、与えられた $b-1$ 次の多項式 $S(x)$ の係数を高次の係数から順次第3の入力Jとなるように、各演算素子1間を接続し、 X^{b-2} での除算を含む多項式 $M(x) = \lambda(x) \cdot S(x) / x^{b-2}$ を演算するものである。

30 【0036】次に、第4の実施例の動作を説明する。

【0037】 $a-1$ 次の多項式 $\lambda(x)$ の1次の係数を λ_1 、 $b-1$ 次の多項式 $S(x)$ のj次の係数を S_j とすると、 $M(x) = \lambda(x) \cdot S(x) / x^{b-2}$ の多項式の乗算は次のアルゴリズムに示すように、各演算素子1の出力がパイプライン的に次の演算素子1に送られて実行される。但し、 $M(x)$ の $r-1$ 次の係数を M_{b-2+r} とし、 $Z_{i,j}$ の初期値は0とする。

【0038】

```

FOR j=1 TO b
  FOR i=1 TO a
    Zi,j = Zi+1,j-1 +  $\lambda_{a-i-1} \cdot S_{b-j}$ 
  NEXT
NEXT
FOR i=1 TO a
  Mb-2+i = Zi,b
NEXT

```

本実施例と第3実施例との違いは、本実施例では $M(x)$ の $b-2$ 次以下の係数を必要としない、即ち、 $M(x) / x^{b-2}$ の演算を実行していることである。第3実施例では $M(x)$ の $b-1$ 次以上の係数 M_{b-2+i} は

7

hクロック後に1番目に配列した演算素子1の出力として一括して得られるので、本実施例は図3の1番目に配列した演算素子1の出力を $Mb-2h$ として表現している。但し、図4はクロック後の出力を表し、それまでの図4の回路の動作は図3の回路の動作と同様である。

【0039】なお、本発明は上述した実施例の他、その要旨の範囲内で種々の変形が可能である。例えば、上記各実施例において、演算素子1として図3に示すように汎用性の高いものを用いて、 $a \cdot b + c \cdot d$ の d として1を入力するようにして $a \cdot b + c$ の演算を行っているが、初めからこの形の演算を行うような演算素子を用いてもよい。また、各々の演算素子のレジスタ及びセレクタを省略した演算素子を用いてもよい。

【0040】

【発明の効果】以上詳述した請求項1記載の発明によれば、複数の演算素子を1次元状のアレイで構成したので、 x^b を法としない一般的な多項式の乗算において、 $\lambda(x)$ の係数が一括して入力される場合でも有効に乗算を行える多項式乗算回路を提供することができる。

【0041】また、請求項2記載の発明によれば、複数の演算素子を1次元状のアレイで構成したので、 x^b を法とする多項式の乗算において、 $\lambda(x)$ の係数が一括して入力される場合でも有効に乗算を行える多項式乗算回路を提供することができる。

【0042】また、請求項3記載の発明によれば、複数の

8

の演算素子を1次元状のアレイで構成したので、 x^b-2 での除算を含まない一般的な多項式の乗算において、 $\lambda(x)$ の係数が一括して入力される場合でも有効に乗算を行える多項式乗算回路を提供することができる。

【0043】また、請求項4記載の発明によれば、複数の演算素子を1次元状のアレイで構成したので、 x^b-2 での除算を含む多項式の乗算において、 $\lambda(x)$ の係数が一括して入力される場合でも有効に乗算を行える多項式乗算回路を提供することができる。

10 【図面の簡単な説明】

【図1】本発明の多項式乗算回路の第1の実施例を示すブロック構成図である。

【図2】本発明の多項式乗算回路の第2の実施例を示すブロック構成図である。

【図3】本発明の多項式乗算回路の第1の実施例を示すブロック構成図である。

【図4】本発明の多項式乗算回路の第2の実施例を示すブロック構成図である。

【図5】本実施例の演算素子のブロック構成図である。

20 【図6】従来の多項式乗算回路のブロック構成図である。

【符号の説明】

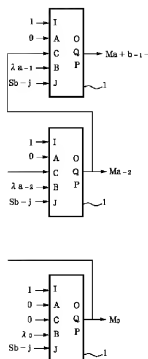
C 第1の入力

B 第2の入力

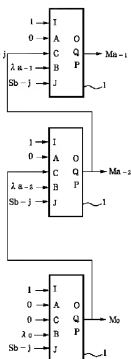
J 第3の入力

1 演算素子

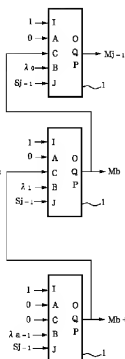
【図1】



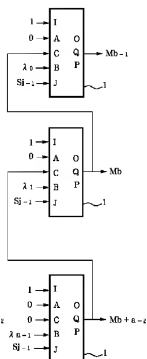
【図2】



【図3】



【図4】



【手続補正書】

【提出日】平成6年6月20日

【手続補正1】

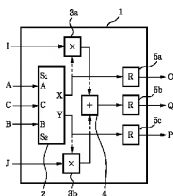
【補正対象書類名】図面

【補正対象項目名】全図

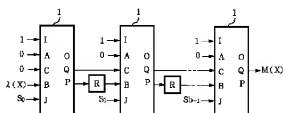
【補正方法】変更

【補正内容】

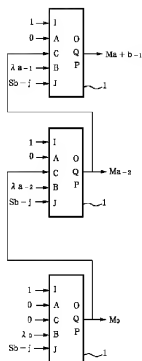
【図5】



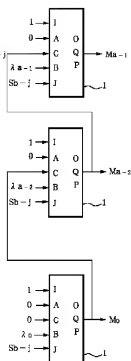
【図6】



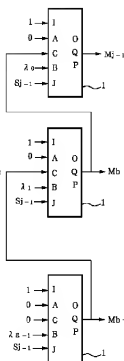
【図1】



【図2】



【図3】



【図4】

